UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/889,126	07/11/2001	Christian Wettergren	64591-64607-EN/CMN	8110

466 7590 03/03/2006

YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/889,126	WETTERGREN, CHRISTIAN	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *7/11/2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

This action is in response to the communication filed on 12/14/2005.

DETAILED ACTION

Response to Arguments

Applicant argues primarily that:

a. The combination of Francisco and Clifton did not disclose that the switches are activated by receiving a signal from the security device.

b. Francisco did not disclose denying the computer processor access to and from the resources or resource ranges selected by the security device.

c. Francisco did not disclose denying access based on any dynamic restriction set by the security processor.

The examiner would first like to point out that in the last paragraph of page 15 of the communication dated 12/14/2005, the applicant appears to have misinterpreted the rejection made in the office action dated 9/14/2005. The applicant has cited a portion of Francisco and argues that this particular section does not disclose what the examiner has claimed it to have disclosed. However, the paragraph cited is not the 3rd paragraph of column 4 as recited in the rejection, but instead it is the 4th paragraph. The correct citation reads "The security system utilizes software in a client/server relationship. The base computer makes requests of the security software. The security software then services these requests and conveys the results to the base computer. From the base computer standpoint, the security software functions like a disk device subsystem."

Regarding applicant's argument a., that the combination of Francisco and Clifton did not disclose that the switches are activated by receiving a signal from the security device, the

examiner does not find the argument persuasive. Francisco clearly disclosed in Col. 5 Paragraph 6 that the access control software was responsible for configuring the AMU hardware. As can be seen in Figs. 1 and 3, the AMU hardware and the access control software were separate from one another and as such in order to "load the look-up tables and control registers of the AMU hardware" the data (signal) that was loaded must have been sent from the access control software to the AMU hardware. As discussed below, it would have been obvious that the access control software was being executed by the security processor 7 and therefore it would have been obvious that the security processor sent the data (signal) which activated the switches. Therefore, the examiner does not find the argument persuasive.

Regarding applicant's argument b., that Francisco did not disclose denying the computer processor access to and from the resources or resource ranges selected by the security device, the examiner does not find the argument persuasive. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, the addition of the teachings of Clifton provide that the secure instructions would only be accessible by the security processor, which would execute the instructions. Therefore, the examiner does not find the argument persuasive.

In response to applicant's argument c., that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., denying access based on any dynamic restriction set by the security processor) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations

from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Therefore, the examiner does not find the argument persuasive.

Because the examiner does not find the arguments persuasive, the examiner has maintained the prior art rejections presented below.

Claims 1-8 have been canceled.

Claims 9-21 have been examined

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 103

Claims 9-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Francisco et al. (US Patent Number 5,263,147) hereinafter referred to as Francisco, and further in view of Clifton (US Patent Number 5,469,556).

Regarding claim 9, Francisco disclosed a system for data processing a security critical activity in a secure management mode in a computer (See Francisco Abstract Lines 6-10), which computer comprises a processor (See Francisco Fig. 1 Element 1), handling devices (See Francisco Fig. 1 Element 25), memory storage means (See Francisco Fig. 1 Element 30), hereafter named resources; that the system comprises a security device (See Francisco Fig. 1 Elements 31 and 100) comprising a processor (See Francisco Fig. 1 Element 7) and signal generators (See Francisco Fig. 3 Element 321), a number of control means, hereafter named switches (See Francisco Fig. 3 Element 325), with signal receivers (See Francisco Col. 5 Paragraph 6 wherein it was inherent that the AMU control had signal generators and the AMU had signal receivers in order for the Control to have configured the AMU) arranged respectively between the security device and the pre-selected resources (See Francisco Fig. 1 Elements 31,

100, and 30), that the switches contain information regarding accessibility to and from the resources, or parts of the resources, hereafter named resource ranges (See Francisco Fig. 1 Element 102 and Claims 1-2), characterized in that the switch controls requests from a processor of the computer, hereafter named the computer processor, to the resources or resource ranges depending on the information contained in the switch (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2), and that in response to a call from the computer processor or the handling devices, the switches are activated by receiving a signal from the security device, said signal from the security device activating the switches to be in a condition (See Francisco Col. 5 paragraph 6) i) enabling the security device access to and from the resources or resource ranges selected by the security device, and ii) denying the computer processor access to and from the resources or resource ranges selected by the security device (See Francisco Col. 4 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject is denied access when they are requesting an access outside the subjects access rights), in that the signal (SG_{PM}) can be generated only by the security device (See Francisco Col. 5 Paragraph 6 Lines 1-4), and in that the security device comprises a signal generator (SG_A), wherein, when a switch receives a signal (SG_A), together with new information (addresses, operation, data), the security device is able of altering a content of the information of that switch (See Francisco Col. 5 Lines 39-50), but Francisco failed to disclose that the security device processor had access to the resources or the security device processor executed the security critical activity.

Clifton teaches that in a computing system it is desirable to have classify certain instructions as secure and others as unsecure and to have a normal processor execute the

unsecure instructions and a secure processor to processor to execute the secure instructions (See Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Clifton in the personal computer security system of Francisco by classifying certain instructions as secure and only allowing the secure instructions to be executed by the security processor. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against the destruction of important data and the compromise of secret or confidential data.

Regarding claim 15, Francisco disclosed a system for data processing a security critical activity in a secure management mode in a computer (See Francisco Abstract Lines 6-10), comprising: a computer comprising a computer processor (See Francisco Fig. 1 Element 1), handling devices (See Francisco Fig. 1 Element 25), memory storage resources (See Francisco Fig. 1 Element 30); a security device (See Francisco Fig. 1 Elements 31 and 100) comprising security device processor (See Francisco Fig. 1 Element 7) and signal generators (See Francisco Fig. 3 Element 321) inputting into the security device processor (See Francisco Col. 2 Lines 22-29 and Col. 5 Paragraph 6); and switch control means (See Francisco Fig. 3 Element 325) comprising switches and signal receivers (See Francisco Col. 5 Paragraph 6 wherein it was inherent that the AMU control had signal generators and the AMU had signal receivers in order for the Control to have configured the AMU), the switches of the switch control means arranged respectively between the security device and pre-selected memory storage resources (See Francisco Fig. 1 Elements 31, 100, and 30), wherein, the switches of the switch control means contain information regarding accessibility to and from the memory storage resources, or ranges

within the memory storage resources (See Francisco Fig. 1 Element 102, and Claims 1-2), the switch control means, depending on the information contained in the switches, controls requests from the computer processor to the memory storage resources or ranges within the memory storage resources (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2), and in response to a call from the computer processor or the handling devices, the switches are activated receiving a control signal from the security device and the security device processor, said control signal activating the switches to be in a condition (See Francisco Col. 5 paragraph 6) i) enabling the security device access to and from the memory storage resources or the ranges within the switch control means memory storage resources selected by the security device and ii) denying the computer processor access to and from the memory storage resources or the ranges within the memory storage resource selected by the security device (See Francisco Col. 4 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject is denied access when they are requesting an access outside the subjects access rights), the control signal (SGPM) can be generated only by the security device (See Francisco Col. 5 Paragraph 6 Lines 1-4), upon any switch receiving a signal (SGA), together with new information (addresses, operation, data), the security device configured to alter a content of the information of that switch (See Francisco Col. 5 Lines 39-50), and the security device processor is a different processor than the computer processor (See Francisco Fig. 1 Elements 1 and 7), but Francisco failed to disclose that the security device processor had access to the resources or the security device processor executed the security critical activity.

Clifton teaches that in a computing system it is desirable to have classify certain instructions as secure and others as unsecure and to have a normal processor execute the

unsecure instructions and a secure processor to processor to execute the secure instructions (See Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Clifton in the personal computer security system of Francisco by classifying certain instructions as secure and only allowing the secure instructions to be executed by the security processor. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against the destruction of important data and the compromise of secret or confidential data.

Regarding claim 16, Francisco disclosed a system for data processing a security critical activity in a secure management mode in a computer (See Francisco Abstract Lines 6-10), comprising: a computer comprising a computer processor (See Francisco Fig. 1 Element 1), connected to handling devices (See Francisco Fig. 1 Element 25) and to memory storage resources (See Francisco Fig. 1 Element 30); a security device (See Francisco Fig. 1 Elements 31 and 100) comprising a security device processor (See Francisco Fig. 1 Element 7) and signal generators (See Francisco Fig. 3 Element 321) inputting into the security device processor (See Francisco Col. 2 Lines 22-29 and Col. 5 Paragraph 6); and switch control means (See Francisco Fig. 3 Element 325) comprising switches and signal receivers (See Francisco Col. 5 Paragraph 6 wherein it was inherent that the AMU control had signal generators and the AMU had signal receivers in order for the Control to have configured the AMU), the switches of the switch control means arranged between the security device and pre-selected memory storage resources (See Francisco Fig. 1 Elements 31, 100, and 30), wherein, the switches of the switch control means contain information regarding accessibility to and from the memory storage resources,

(See Francisco Fig. 1 Element 102, and Claims 1-2), the switch control means, based on the information contained in the switches, controls requests from the computer processor to the memory storage resources (See Francisco Fig. 1 Element 102, Col. 2 Paragraphs 2-3, and Claims 1-2), and in response to a call from the computer processor, the switches are activated by receiving a control signal from the security device and the security device processor, said control signal activating the switches to be in a condition (See Francisco Col. 5 paragraph 6) to i) enable the security device access to and from the memory storage resources selected by the security device and ii) deny the computer processor access to and from the memory storage resources selected by the security device (See Francisco Col. 4 Paragraph 3 and Claim 1 wherein the AMU has access to the requested memory, and the subject is denied access when they are requesting an access outside the subjects access rights), the control signal (SGPM) can be generated only by the security device (See Francisco Col. 5 Paragraph 6 Lines 1-4), upon any switch receiving a signal (SGA), together with new information (addresses, operation, data), the security device configured to alter a content of the information of that switch (See Francisco Col. 5 Lines 39-50), and the security device processor is a different processor than the computer processor (See Francisco Fig. 1 Elements 1 and 7), but Francisco failed to disclose that the security device processor had access to the resources or the security device processor executed the security critical activity.

Clifton teaches that in a computing system it is desirable to have classify certain instructions as secure and others as unsecure and to have a normal processor execute the unsecure instructions and a secure processor to processor to execute the secure instructions (See Clifton Col. 1 Lines 19-25, Col. 4 Lines 6-65, and Col. 5 Lines 25-45).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Clifton in the personal computer security system of Francisco by classifying certain instructions as secure and only allowing the secure instructions to be executed by the security processor. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect against the destruction of important data and the compromise of secret or confidential data.

Regarding claim 10, the combination of Francisco and Clifton disclosed that the information contained in the switches controls access to resources for requests from other possible processors contained in or connected to the computer (See Francisco Col. 6 line 68 – Col. 7 Line 4).

Regarding claim 11, the combination of Francisco and Clifton disclosed that the switches comprise a signal receiver by which it can detect which source is handling the computer, and that the switch compares this with the resource which requests access to a resource or resource range controlled by the switch, and depending on the information in the switch, enables or denies access to that resource (See Francisco Fig. 2b).

Regarding claim 12, the combination of Francisco and Clifton disclosed that the information in the switch enables the switch to control certain areas of the memory means are allocated to be accessed by the processor of the security device only (See Francisco Col. 4 Paragraph 3).

Regarding claim 13, the combination of Francisco and Clifton disclosed that the information in the switch enables the switch to control that certain resources are accessible by the computer processor when not in secure management mode, and only accessible by the

security device when in secure management mode (See Francisco Col. 2 paragraph 3 wherein the large address space mode constituted the non-secure mode and the segmented address space constituted the secure mode).

Regarding claims 14, and 17-18, the combination of Francisco and Clifton disclosed that the switches are hardware switches (See Francisco Fig. 4 Element 325), the switches configured for i) a first normal mode wherein the computer processor has access to the resources, and ii) a second protected mode wherein the computer processor is denied access to the resources and the security processor is allowed access to the resources (See the rejection of claim 9 above), and said signal from the security device, enabling the security device and the security processor access to the resources and denying the computer processor access to the resources, changes the switches fro the first normal mode into the second protected mode (See the rejection of claim 9 above and Francisco Col. 5 paragraph 6).

Regarding claims 19-21, the combination of Francisco and Clifton disclosed the switches each comprise a protection mode signal receiver configured to receive said signal from the security device activating the switches to be in the condition enabling the security device and the security processor access to the resources and denying the computer processor access to the resources (See the rejection of claim 9 above, and Francisco Col. 5 paragraph 6 wherein it was inherent that the AMU hardware contain "signal receivers" in order to have received the configuration messages), upon reception of said signal from the security device by the protection mode signal receiver, the protection mode signal receiver reconfigures the switches into a protection mode configuration allocating specific resources needed for executing the security critical activity to the security processor and denying the computer processor access to the

specific resources (See the rejection of claim 9 above, Francisco Col. 5 paragraph 6), and upon the switches being placed in the protection mode configuration, the security processor executes the security critical activity (See the rejection of claim 9 above).

Conclusion

Claims 1-8 have been have been canceled and claims 9-21 have been rejected..

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
2/26/2006

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100